

SnapFense:

Managed and Interoperable Secure Network Solution

Snap Defense Systems reserves the right, without notice, to make changes in equipment design or specifications.

Snap Defense Systems will make every effort to provide accurate and reliable information. However, Snap Defense Systems assumes no responsibility for its use or for rights of third parties, which may result from its use.

Any representations in this document concerning performance are for informational purposes only and are not warranties of future performance either express or implied. Snap Defense Systems standard limited warranty stated in its sales contracts, order confirmation form or any other document, is the only warranty offered by Snap Defense Systems.

This document contains proprietary information. Neither this document nor said proprietary information, nor any part thereof, shall be published, reproduced, copied, disclosed, or used for any purpose other than the review and consideration of this material without written approval from Snap Defense Systems.

Trademarks

Snap Defense Systems, **SNAP**, **Snapfone**, **Snapcell**, **Snapsoft**, **Snaptrunk**, **Snapmaster**, **Snapgate**, **SnapMesh**, **SnapFence**, **SnapZone**, **Snaploader**, and **STconsole** are trademarks of Snap Defense Systems LLC. Windows and Microsoft TM are trademarks of Microsoft Corporation, Dialogic is a trademark of Dialogic Corporation. All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark. All trademarks mentioned hereby belong to their respective owners.

Snap Defense Systems LLC

Table of Contents

1	THE CONCEPT	5
2	SNAPFENSE MAIN COMPENENTS.....	6
2.1	Call Flow Explained	6
2.1.1	<i>SnapFense</i> subscriber calls a non-subscriber	7
2.2	Non-subscriber calls a <i>SnapFense</i> subscriber	8
2.3	<i>SnapFense</i> subscriber to another <i>SnapFense</i> subscriber	10
2.4	Calls between Snaptrunks.....	11
2.5	Digital Encryption	12
2.6	Snapcrypt.....	12
2.6.1	Snapcrypt Features.....	12
3	SNAPFENSE ELEMENTS	13
3.1	Snaptrunk - Secure Communications Gateway.....	13
3.1.1	Description	13
3.1.2	Snaptrunk as a Network Switch.....	14
3.2	STconsole – Management Console.....	15
3.2.1	Description	15
3.2.2	Features	15
3.2.3	Remote Connection	15
3.3	Snapsoft Security Software.....	16
3.3.1	Snapsoft Features	16
3.4	Snapfone	17
3.4.1	Snapfone Features	17
4	SNAPFENSE SYSTEM FEATURES.....	18
4.1	Lawful Interception (LI) & CALEA Compliance	18
4.1.1	Call Flow with LI (Example).....	18
4.2	Direct Dialing	18
4.3	Call Drop Errors & Normal releases.....	19
4.4	Alarms 19	
4.4.1	Failure Situations	19
4.4.2	Alert Mechanisms	19
4.5	Secure Data Modem Support - Option	Error! Bookmark not defined.
5	APPENDIX A.....	20
6	SNAPFENSE SYSTEM SPECIFICATIONS	21
6.1	Snaptrunk Hardware	21
6.1.1	Snaptrunk Specifications.....	21
6.2	Snaptrunk Software	21
6.2.1	Vocoder	21
6.2.2	Encryption (FIPS compliant).....	21
6.2.3	Modem 21	
6.2.4	V110.....	21
6.2.5	V32.....	21
6.2.6	Fax Relay	21
6.3	Snapfone Hardware	22
6.3.1	Approvals	22
6.3.2	Supported Line Parameters	22
6.3.3	DTMF Signaling	22
6.3.4	Line Interface Parameters (DAA)	22
6.3.5	Phone Interface Parameters (SLIC)	22
6.3.6	Miscellaneous.....	22

CONFIDENTIAL

6.4	Snapfone Software	23
6.4.1	Modem	23
6.4.2	Vocoder	23
6.4.3	Encryption (FIPS compliant).....	23
6.4.4	Fax Relay	23
6.5	Snapsoft Software	23
6.5.1	V110.....	23
6.5.2	V32.....	23
6.5.3	Fax Relay	23
6.5.4	Vocoder	23
6.5.5	Encryption (FIPS compliant).....	23
7	TERMINOLOGY	24

1 The Concept

Snap Defense Systems has developed a robust, scalable and cost-effective interoperable encryption solution into a single security platform. The company's architecture is; SNAP (Secure Network Access Platform) which is a point-to-multipoint total security solution. It is the only unified, interoperable, and secure telephony communications platform available for both government and commercial applications. The unique architecture is revolutionary because the main security functions are deployed, managed and enforced through a network-based security gateway versus other products whose primary security functions are end-user controlled at the end-points. Through the network-based concept we can provide security to any SNAP subscriber even when only one party has an encryption device. This allows the subscriber to have security at all times instead of only when both parties have a similar encryption device.

The **SnapFense** total security solution provides enterprise users with security features, such as authentication, access control, user calling restrictions, VPN encryption, call destination encryption and point-to-any-point secured communications. The solution also uses a variety of off-the-shelf devices for transparently securing the user's end-point's voice, fax or data.

The hub known as the **Snaptrunk** is connected to E1/T1 digital trunks. The **Snapfone** is connected through POTS lines. Both the **Snapcell** & **Snapsoft** are used for connecting through wireless carriers. **SnapFense** Main Components



CONFIDENTIAL

2 SnapFense Main Components

The main components of the **SnapFense** solution are: 1) Network Equipment- **Snaptrunk**, 2) End-points- **Snapfone**, **Snapcell** and **Snapsoft**, and 3) Management Software - **STconsole**. For the purposes of IWN: **Snapfone** & **Snapsoft** will be the preferred end-points.

- ♦ The **Snapfone**, **Snapcell** and **Snapsoft** are encryption end-point units. The **Snapfone** plugs in between a telephone (or a fax machine) and the RJ-11 line port. The **Snapsoft** is an embedded software application that provides encrypted voice, text and data security on a handheld mobile device. The **Snapcell** is a hardware plug-in for Sony-Ericsson phones that provides voice security.
- ♦ The **Snaptrunk** is a multi-line encryption gateway connected to the PSTN via digital interfaces such as E1/T1 ISDN PRI trunks. Installed at a point-of-presence, the **Snaptrunk** encrypts/decrypts communications to/from the end-points. It acts as the hub for all network activity.
- ♦ The **STconsole** is an enterprise management software for performing remote management, enforcing policies to end-points and maintaining a database of all subscribers within the **SnapFense** network.

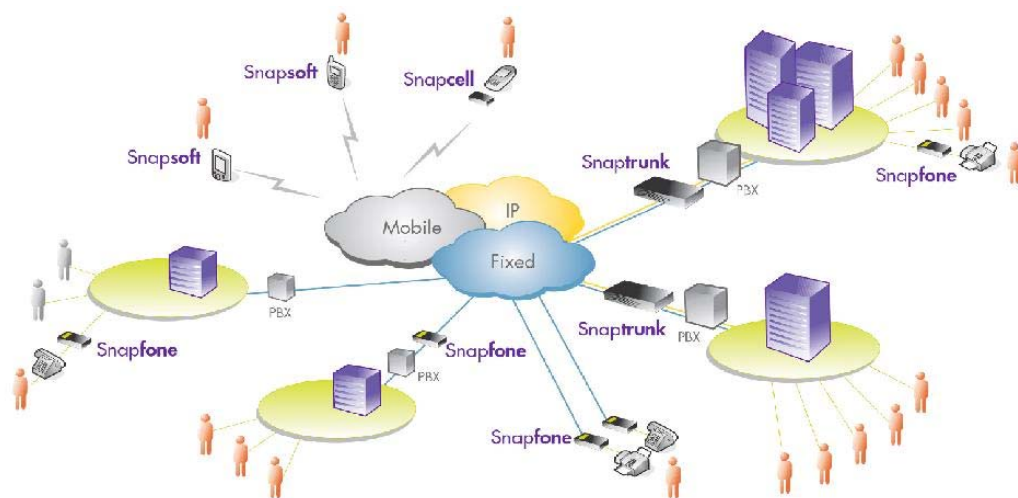


Figure 1 **SnapFense**- Interoperable Secure Network (ISN)

2.1 Call Flow Explained

Figure 1 pictures the **SnapFense** solution for Interoperable Secure Network (ISN)

- ◆ All calls for subscribers of the **SnapFense (ISN)** are logically routed through one or more **Snaptrunks** depending on user definitions.
- ◆ All communications between a **Snaptrunk** and a End-point will always be secured, regardless to which side is equipped with a **Snapfone**.
- ◆ The End-Points provide the necessary information to the **Snaptrunk** for user authentication, and **Snaptrunk** is the component that analyzes this information and carries out the necessary switching and routing to establish an End-to-End secure call or a Secure-to-Network only connection.
- ◆ The procedure for call-setup, routing and access depend on which of the two parties is a subscriber of the **SnapFense (ISN)**. There are three different possible scenarios for Secure Call Setup: 1) Subscriber calls a non-subscriber; 2) Non-subscriber calls a subscriber's secure number, 3) Two subscribers call each other.

Note:

The Gray colored areas in the tables 1-4 relate to procedures taking place between the **Snaptrunk** and the **Snapsoft** or **Snapfone** during different stages of the secured channel setup. See "Appendix A" for additional call flow diagram.

2.1.1 SnapFense subscriber calls a non-subscriber

For convenience, we identify this scenario as a User – to – Non-User Call.

Diagram 1 illustrates the step-by-step interactions among the **SnapFense** components. The technical explanation of each phase is in greater detail within **Table 1 User-to-Non-User Call Explained**.

Diagram 1 User-to-Non-User Call Flow

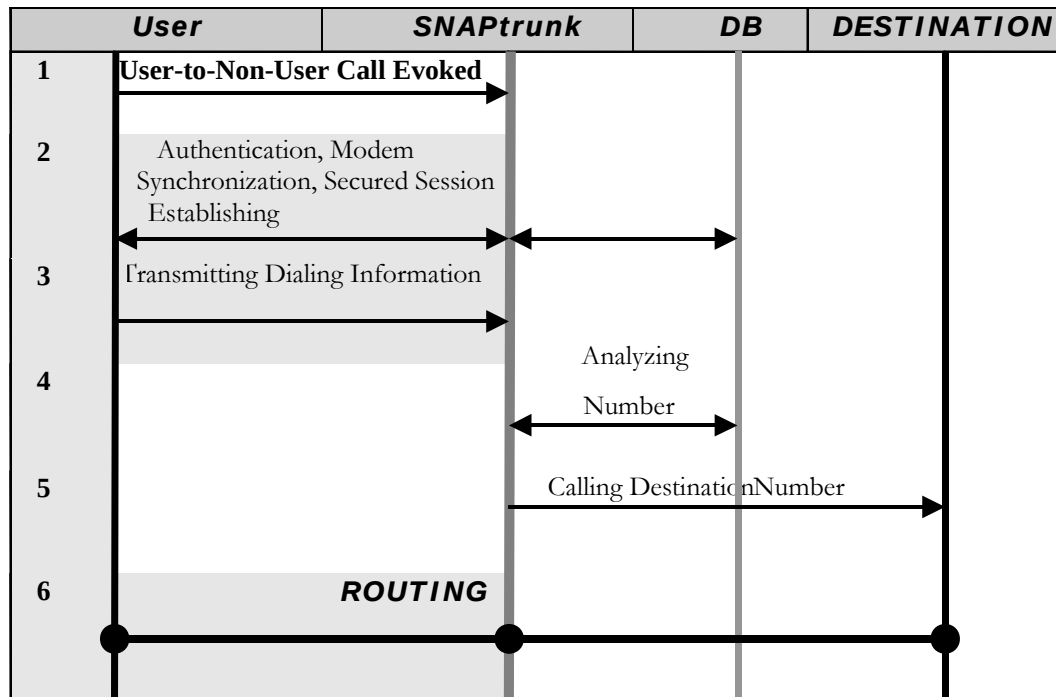


Table 1 User-to-Non-User Call Explained

1	SnapFense user wants to make a secure call using an encryption end-point (Snapfone , Snapcell , or Snapsoft). The user dials the destination number. The end-point transparently dials to the Snaptrunk using
---	--

	a dedicated gateway telephone number that is preprogrammed into the software or hardware encryption end-point by their administrator. While the unsecure channel is being converted into an encrypted channel, the actual destination number is stored in the end-point's memory. For Snapsoft and Snapcell on GSM networks: The mobile phone will communicate with carrier's switch and through AT commands a request for CSD bearer services is made. The commands can be for a transparent or non-transparent data call using a bit rate of 9600 bps. In the signaling phase there is a request from the IWF (inter-working function) to allocate a V.32 or V.110 modem session. The call from the IWF is then routed to the Snaptrunk through PRI line (The Snaptrunk accepts the call and uses the correct modem to establish a data channel connection). All voice and encryption processes will be transparent to network.
2	The Snapfone, Snapcell or Snapsoft and the Snaptrunk start a session based on the v.32/ v.110 protocol or a regular modem session followed by a key exchange. Upon successful synchronization, key exchange, and <i>end-point</i> authentication, within the database, the Snaptrunk initiates an encrypted channel between itself and the subscriber's end-point device.
3	The channel is now encrypted. The end-point device transmits the actual destination number to the Snaptrunk .
4	The Snaptrunk queries the internal user database to determine whether the destination number is registered to a SnapFense user, as well as the privileges and credentials of the user.
5	In this example, the destination is not registered to a SnapFense user and the user is authorized to make outgoing calls to non-users. The Snaptrunk generates an outbound call using the destination number on a different channel on the E1 trunk.
6	Both channels are logically routed and connected. The user's access network will be totally secure. The subscriber is notified visually and audibly of the security level achieved prior before both parties can start communicating.

Note: The system compresses voice to 8 Kbit/sec (G-729A) for Snapfone and 6.4Kbit/sec (G723.1) for Snapcell & Snapsoft PDA while retaining a high voice quality (toll quality) and uses fax relay for fax transmissions. The initial call setup time is about 6 to 7 seconds. The round trip delay is less than 100msec for Snapfone and about 400msec for Snapcell or Snapsoft PDA. The voice is toll-quality over both wireless and wired networks.

2.2 Non-subscriber calls a SnapFense subscriber

For convenience, we identify this scenario as a Non-User-to-User call.

Diagram 2 Non-User-to-User Call Flow, accompanied by **Table 2 Non-User-to-User Call explained**, illustrates this scenario.

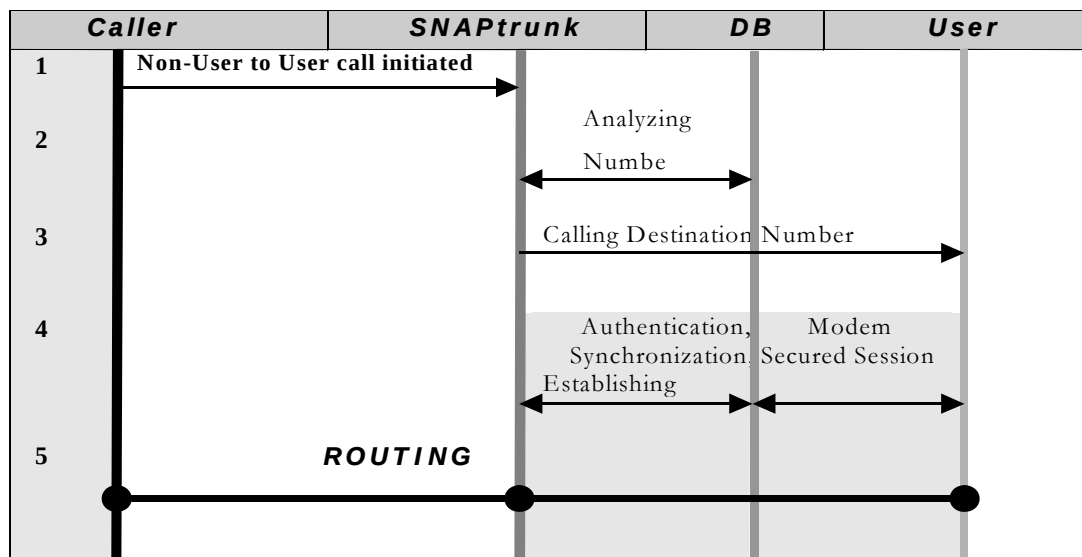


Diagram 2 Non-User-to-User call flow

Table 2 Non-User-to-User call explained

1	The secure number of a SnapFense subscriber is dialed. The call is routed to a Snaptrunk first..
2	The Snaptrunk queries the internal user database to determine whether the destination number is registered to a SnapFense user, as well as the privileges and credentials of the user.
3	The Snaptrunk dials the real destination number on different channel on the E1 or T1 trunk.
4	The Snaptrunk and the destination end-point device (Snapfone , Snapcell or Snapsoft) begin a modem session followed by key exchange. Upon successful synchronization, key exchange, and user authentication within the internal Snaptrunk database, the Snaptrunk initiates an outbound encrypted channel between itself and the end-point device (Snapfone Snapcell or Snapsoft).
5	Both channels are logically routed and connected. The user's access network will be totally secure. The subscriber is notified visually and audibly of the security level achieved prior before both parties can start communicating.

CONFIDENTIAL

2.3 SnapFense subscriber to another SnapFense subscriber

This scenario describes a User-to-User call.

Diagram 3: User-to-User call flow illustrates the secured connections on both segments from a subscriber to the **Snaptrunk**, and from the **Snaptrunk** to another subscriber.

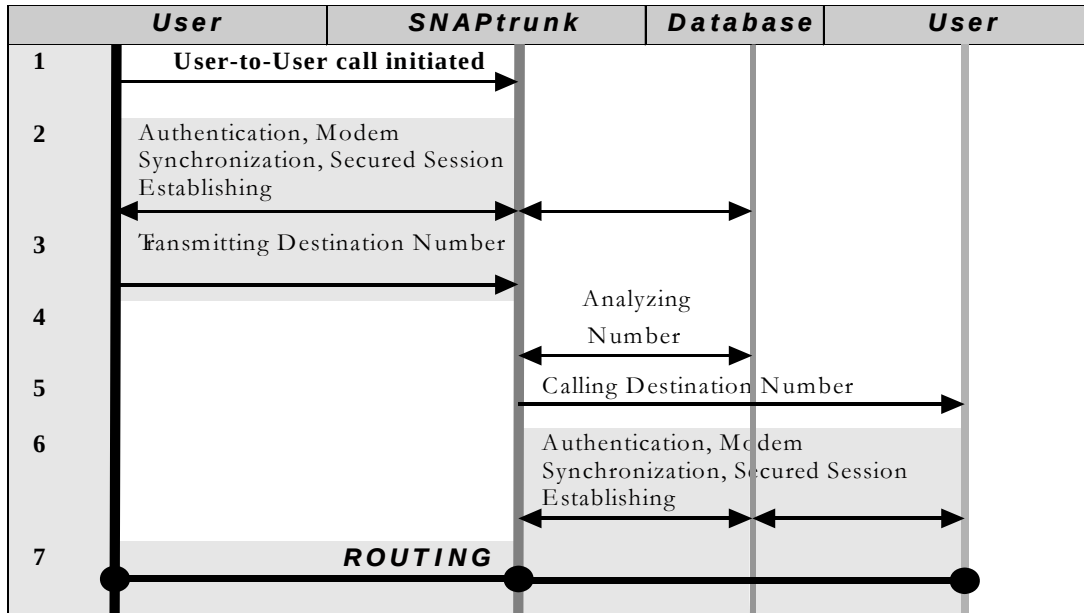


Diagram 3 User -to-User call flow

Table 3 User-to-User call explained

1	SnapFense user makes a secure call using an encryption end-point (Snapfone , Snapcell , or Snapsoft). The user dials the destination number. The end-point transparently dials to the Snaptrunk using a dedicated gateway telephone number that is preprogrammed into the software or hardware encryption end-point by their administrator. While the unsecure channel is being converted into an encrypted channel, the actual destination number is stored in the end-point's memory. For Snapsoft and Snapcell on GSM networks: The mobile phone will communicate with carrier's switch and through AT commands a request for CSD bearer services is made. The commands can be for a transparent or non-transparent data call using a bit rate of 9600 bps. In the signaling phase there is a request from the IWF (inter-working function) to allocate a V.32 or V.110 modem session. The call from the IWF is then routed to the Snaptrunk through PRI line (The Snaptrunk accepts the call and uses the correct modem to establish a data channel connection). All voice and encryption processes will be transparent to network.
2	The Snapfone , Snapcell or Snapsoft and the Snaptrunk initiate a session based on the v.32/ v.110 protocol or a regular modem session followed by a key exchange. Upon successful synchronization, key exchange, and <i>end-point</i> authentication (within the database) the Snaptrunk initiates an encrypted channel between itself and the subscriber's end-point device.
3	The channel is now encrypted. The end-point device transmits the actual destination number to the Snaptrunk .
4	The Snaptrunk queries the internal user database to determine whether the destination number is registered to a SnapFense user, as well as the privileges and credentials of the user.
5	The Snaptrunk generates an outbound call to the end-point device using the real number on a different channel on the E1 or T1 trunk.
6	The Snapfone , Snapcell or Snapsoft and the Snaptrunk initiate a session based on the v.32/v.110 protocol or a regular modem session followed by a key exchange. Upon successful synchronization, key exchange, and <i>end-point</i> authentication, within the database, the Snaptrunk initiates an encrypted channel between itself and the subscriber's end-point device at the destination.
7	Both channels are logically routed and connected. The user's access network will be totally secure. The subscriber is notified visually and audibly of the security level achieved prior before both parties can start communicating.

2.4 Calls between Snaptrunks

This scenario describes a User-to-User Call with two different **Snaptrunks** in two different locations (please refer to Figure 1, Appendix A, Diagram 4) where two **Snaptrunks** are connected to PBX's. In this example the **Snaptrunks** performs two duties; as a security gateway and telecommunications firewall by protecting the PBX's from brute-force and rouge modem attacks.

The subscribers in this scenario do not have an end-point device (**Snapsoft**, **Snapcell** or **Snapfone**) The synchronization occurs between two **Snaptrunks**. The connection between both facilities will be secured every time a subscriber calls from/to either facility.

Diagram 4 Snaptrunk - to - Snaptrunk Call Flow

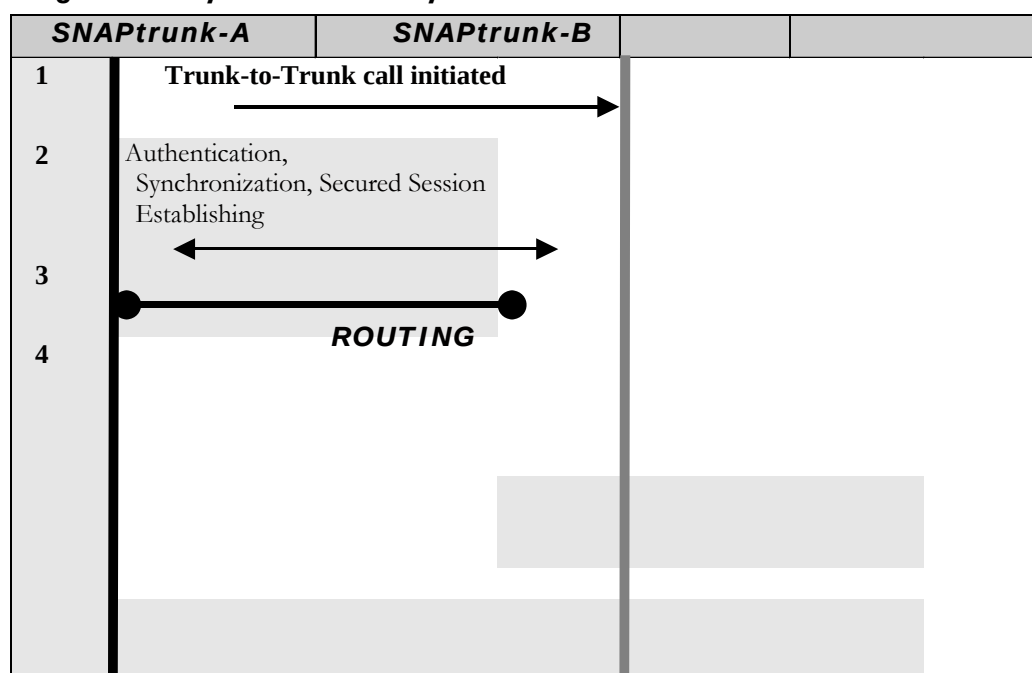


Table 4 Snaptrunk to Snaptrunk call Explained

1	User dials the destination number.
2	Snaptrunk-A encrypts the call and sends it to PSTN secured.
3	The channel is now secure.
4	Snaptrunk-B accepts the call, synchronizes with Snaptrunk-A , and decrypts the call.
5	Other user accepts the call.

Note:

The **Snaptrunk** operates the E1/T1 interface as a 30/24 individual time slot of voice information. The output port leaving one destination is designated to the input port of other **Snaptrunk**. This occurs as a 64K encryption/decryption session after the ADPCM compression. The initial call setup time is approximately 1.5 seconds. Round trip delay is less than 40msec. The transport link between **Snaptrunks** is secured. Internet protocol for data call is currently not supported. It will be available as an upgrade.

2.5 Digital Encryption

The **SnapFense** total security architecture implements both public and high fidelity private key encryption technologies.

The 3DES/AES and 1024-bit Diffie-Hellman algorithms constitute the core of the current encryption process. The 1024-bit Diffie-Hellman algorithm is used for key exchange and authentication at the beginning of a session. The system implements the 3DES/AES algorithm for encrypting the actual session. New keys are drawn for each session. The flexible design allows implementation of other encryption algorithms as an option. The **SnapFense** system encryption level can be easily upgraded, even remotely.

2.6 Snapcrypt

Snapcrypt enables rapid and robust implementation of security applications in embedded systems. Powered by industry-standard cryptographic algorithms and optimized for mobile applications. Snapcrypt addresses security requirements by offering cryptographic libraries optimized for Texas Instruments DSP and for ARM RISC processors. Snapcrypt features a small memory footprint combined with exceptional efficiency that minimizes the impact on battery life. Snapcrypt provides a complete suite of industry standard cryptographic libraries. These cryptographic libraries enable application developers to easily integrate encryption, hash functions, digital signatures and key exchange mechanisms into embedded systems.



Snapcrypt core engines are FIPS approved which means that the protocols, algorithms and key management processes meet and/or exceed government standards for protecting up to the most sensitive user information. Snap Defense Systems also offers software which can create interoperability among different devices. This, in turn, creates operational efficiencies and reduced capital expenditures when procuring secure communication systems.

Snapcrypt provides various private and public key encryption algorithms including all algorithms required by the IPSec standard, such as DES, 3DES and AES for symmetric encryption, key exchange protected by ElGamal, RSA and Diffie-Hellman, MD5 and SHA-1 hash functions, along with their keyed versions (HMAC), RSA, ECC and DSA for digital signatures.

2.6.1 Snapcrypt Features

- Advanced cryptographic cores approved by NIST
- DSP optimization with batter-saving technology
- High performing and efficient engines
- Small footprint design
- Fast turn around to market, greater return on investment

3 SnapFense Elements

3.1 Snaptrunk - Secure Communications Gateway



Figure 2 **Snaptrunk**

3.1.1 Description

The **Snaptrunk** is a security encryption gateway with enterprise management software. It is connected via digital circuits (T1/E1 or ISDN) and the PBX. **Snaptrunk** is a security breakthrough in communications. It shifts the security administrative controls to the network level, rather than the individual user. This allows for greater continuity across the enterprise, improved compliance with security policies and centralization of administrative controls. For example, **Snaptrunk** includes central management functionality capable of supporting and managing groups of secured networks and performing management services, such as authentication, configuration, alarm, statistics, user profiling, auditing, call detail reports (CDR), remote upgrading and more. **Snaptrunk** is also compatible with all major PBX manufactures.

Snaptrunk is an effective tool that enforces and monitors corporate security policy by detecting, logging and controlling all inbound and outbound network activity based on user-defined, automated security policies. It protects enterprise networks, phone systems and other critical infrastructure from back-door and other external attacks through the Public Switched Telephone Network (PSTN). Additionally, the **Snaptrunk** also securely connects users at endpoints using **Snapsoft**, **Snapcell**, and **Snapfone** with each other.

The **Snaptrunk**'s super-advanced gateway architecture is based on military technology used for protecting battlefield and military intelligence. **Snaptrunk** is completely transparent to the end-user, allowing a secure call to be placed in the exact same manner as a regular call. **Snaptrunk** is also capable of securing conference calls and with its patented multipoint switching technology can protect remote users from any location regardless of connectivity (analog, digital or cellular). A single **Snaptrunk** can support up to six E1/T1 interfaces, securing up to 180 concurrent secure calls which can typically secure up to 1800 users. Multiple **Snaptrunks** can be rack-mounted for additional capacity.

3.1.2 Snaptrunk as a Network Switch

All the digital trunks at a **SnapFense** node should be of the same range of telephone numbers (“node range”). Any number dialed within this range reaches a **Snaptrunk** at the node. The routing to one trunk or the other is dependent on the Telecom Operator’s algorithm and configuration.

A call can reach a **Snaptrunk** for one of the following reasons:

1) **A user initiates a secure call:**

Snapfones, **Snapcells**, and **Snapsofts** can be registered to one or more **Snaptrunks**. The user never dials the Snaptrunk’s Security Center telephone number as the units are preconfigured to dial a specific telephone number within the node’s range of numbers.

2) **A non-user dials a number associated with a subscriber:**

The “association” can be one of the following:

- **Using Secure Numbers:**

The administrator supplies each user with a unique secure virtual number within the range of the **SnapFense** node. When a call is placed to a secure virtual number the **Snaptrunk** retrieves the real number from the database and dials it generates an outbound secure session.

- **Using a dedicated Service Provider prefix:**

The telecom operator may provide the organization with a dedicated prefix. Any call starting with this prefix will be routed to the associated **Snaptrunk** site. The **Snaptrunk** then removes the prefix from the dialed number, and dials the remaining digits for the secure call.

3.2 STconsole – Management Console



Figure 1: Main Window
STconsole interface

3.2.1 Description

The **SnapFense** system architecture provides user-friendly enterprise management software; the **STconsole**.

STconsole provides several administrative tools for managing all security aspects for registered subscribers of the **SnapFense** solution. **STconsole** is equipped to monitor each **Snaptrunk's** status, call traffic, audit records, as well as enterprise policy enforcement, updating device parameters and key management.

The **SnapFense** database stores registered user details, Call Detail Reports (CDR), node configuration data, and other information. Over 200 parameters can be defined, managed and controlled.

STconsole management software is compatible with Windows™ operating systems. **STconsole** can be connected to a **Snaptrunk** via LAN, or RAS (through a modem); using an authorized account, an administrator may remotely control the **SnapFense** nodes according to administrative privileges.

3.2.2 Features

- Administrative database for managing registered subscribers
- Ability to deactivate lost or stolen units
- Register end-user devices on **SnapFense** network
- Define user & group credentials
- Manage large networks with thousands of users in multiple locations
- Policy enforcement to encryption end-points

3.2.3 Remote Connection

RAS: **SnapFense** can be reached via a POTS line using Remote Access Server (through a dial up modem) with username and password protection.

Internet: Organizations that choose to make **SnapFense** accessible via the Internet will be responsible for providing required security elements (firewalls, routers, etc).

3.3 Snapsoft Security Software

Snapsoft is a software solution for securing voice and data security communications that use GSM based networks. **Snapsoft** is transparent and compatible with Commercial Off-the-Shelf (COTS) Smartphones, such as HP's IPAQ, I-Mate phones, Siemens and several other devices.



Because it is compatible with COTS devices it can be downloaded into the device from a PC. This eliminates the need for a hardware dongle or an expensive proprietary handset. Using high performance encryption libraries the **Snapsoft** software is built on security standards approved by the U.S. National Institute of Standards and Technology (NIST). **Snapsoft** uses advanced battery-saving technology which minimizes the impact on batteries while providing a high performance solution that delivers high quality encrypted voice communications.

Snapsoft ensures that all information residing on a device (data at rest) can be encrypted and controlled with user-defined criteria. In addition, **Snapsoft** offers secure data connectivity (data in motion) for all popular forms of messaging and connectivity (VPN, email, SMS, MMS, file transfer, chat, etc.). **Snapsoft** is compatible with Smartphones and PDA's using operating systems such as Windows Mobile, Symbian, Palm and Linux (Q3-2006).

Snapsoft can be downloaded into the device from a PC via ActiveSync software. **Snapsoft** is easy to use and does not require extensive user training. As with all SNAP solutions the **Snapsoft** can be incorporated, configured and administered as part of the **SnapFense** solution for maximum compliance with all security policies across the entire enterprise.

3.3.1 Snapsoft Features

- Highest Security Certification (FIPS 140-2 level 2)
- Transparent and user-friendly
- Complete voice and data security solution (data at rest and in motion)
- Compatible with all four GSM frequencies and networks
- Battery saving technology
- Advanced point-to-multipoint technology (upgrade)
- Advanced management features (upgrade)
- Enterprise user control (upgrade)

3.4 Snapfone

The **Snapfone** is a plug and play Customer Premise Equipment (CPE) unit, connected between an analog telephone or fax machine and a RJ-11 connection port.

Snapfones can be is preprogrammed by the organization's administrator to auto-dial the **Snaptrunk's** security center number during the initial call setup. This telephone number is preconfigured while the "dialed" destination number is user defined for the outgoing secure call being established by the **Snaptrunk**. A modem session is created for every connection between a **Snapfone** and a **Snaptrunk**, regardless of who originates the call from within or outside the **SnapFence** solution. After both **Snapfone** and **Snaptrunk** successfully synchronize, a key exchange session is established using Diffie-Hellman and 3DES/AES secure link is established. When a **Snapfone** has created a secure link with the **Snaptrunk**, it is only then that the **Snapfone** will transmit the destination number to the **Snaptrunk**. The **Snaptrunk** then generates the outgoing call to the other party. This added level of security prevents the hostile capture of the destination number.



The **Snapfone's** software can be programmed and upgraded at the factory, remotely, or via a RS232 connection to PC. The **Snapfone** can be controlled and operated remotely via DTMF. Bi-directional DTMF and signaling bits to the carrier are transferred transparently.

3.4.1 Snapfone Features

- Highest Security Certification (FIPS 140-2 Level 2)
- Minimal voice latency
- Transparent and user-friendly experience
- Compatible with COTS telephone and fax machine
- Remote update and maintenance capability (optional)
- Enhanced management features (optional)
- Advanced point-to-multipoint technology (optional)
- Compatible with ISDN (requires terminal adapter)
- Compatible with INMARSAT (GAN) technology (requires terminal adapter)

4 SnapFense System Features

4.1 Lawful Interception (LI) & CALEA Compliance

The **SnapFense** system may be subject to domestic law regulations regarding the Lawful Interception (LI) of telecommunication traffic. In order to meet the Law Enforcement Agencies' (LEA) needs to monitor specific conversations, **SnapFense** provides the **Call Diversion to Voice Logger** feature.

One of the two monitoring models may be adopted:

1. The **Snaptrunk** transfers the encrypted communication to the Law Enforcement Monitoring Facility (LEMF) that is supplied with a similar **Snaptrunk** and/or components; **Snapfone**, **Snapcell**, **Snapsoft** for decrypting;
2. The **Snaptrunk** transfers the non-encrypted conversation to the LEMF.

Snap Defense Systems can customize the necessary components to meet the requirements of Law Enforcement agencies.

4.1.1 Call Flow with LI (Example)

Prior to making an outbound call, **Snaptrunk** checks if the subscriber or encryption end-point are subject to LI.

The **Snaptrunk** retrieves the Voice Logger number from the database and calls telephone number of the Law Enforcement agency prior to connecting the destination party.

1. When the **Snaptrunk** establishes a connection with the Voice Logger, it:
 - a. Sends header information as defined by the authorities (caller, destination party, S/N);
 - b. Continues the normal call flow (dials to the destination and routes);
 - c. Transfers the conversation or fax transmission to the LEMF, uncompressed.
2. If the **Snaptrunk** does not succeed in establishing connection with the LEMF, it stops the call flow, does not call the destination, and drops the caller.

Note:

If both parties are subject to LI to the same LEMF, the procedures described above are performed only once.

4.2 Direct Dialing

Within an organization or a group it may be essential to maintain secured point-to-point connections without having to reach the **Snaptrunk**. The **Snapfone** may be preprogrammed with a list of up to 50 telephones or fax numbers. If a telephone or fax number is dialed that matches an entry of the list (fully or just as prefix), your **Snapfone** will not dial to the **Snaptrunk**, but will try to connect directly to the destination **Snapfone** and establish a secure connection with it.

For example, if "7666540" is dialed, and "766" is included in the list, your **Snapfone** will dial directly the destination **Snapfone** and start a secure session with it.

Implementation of this feature depends on your configurations and software version. Please refer to **Snapfone User Manual** for additional details.

4.3 Call Drop Errors & Normal releases

Upon every call termination the database records the termination codes for both incoming and outgoing calls.

4.4 Alarms

Alert will be triggered as result of a failure and recorded within the **STconsole**.

4.4.1 Failure Situations

Database failure

UPS alert (UPS should be plugged to **Snaptrunk** machine)

Any E1/T1 Layer 2 alarm (e.g. loss of synchronization)

PSecure board fails to synchronize with **Snapfone, Snapsoft**

Unauthorized **Snaptrunk** termination (watchdog application will also block E1).

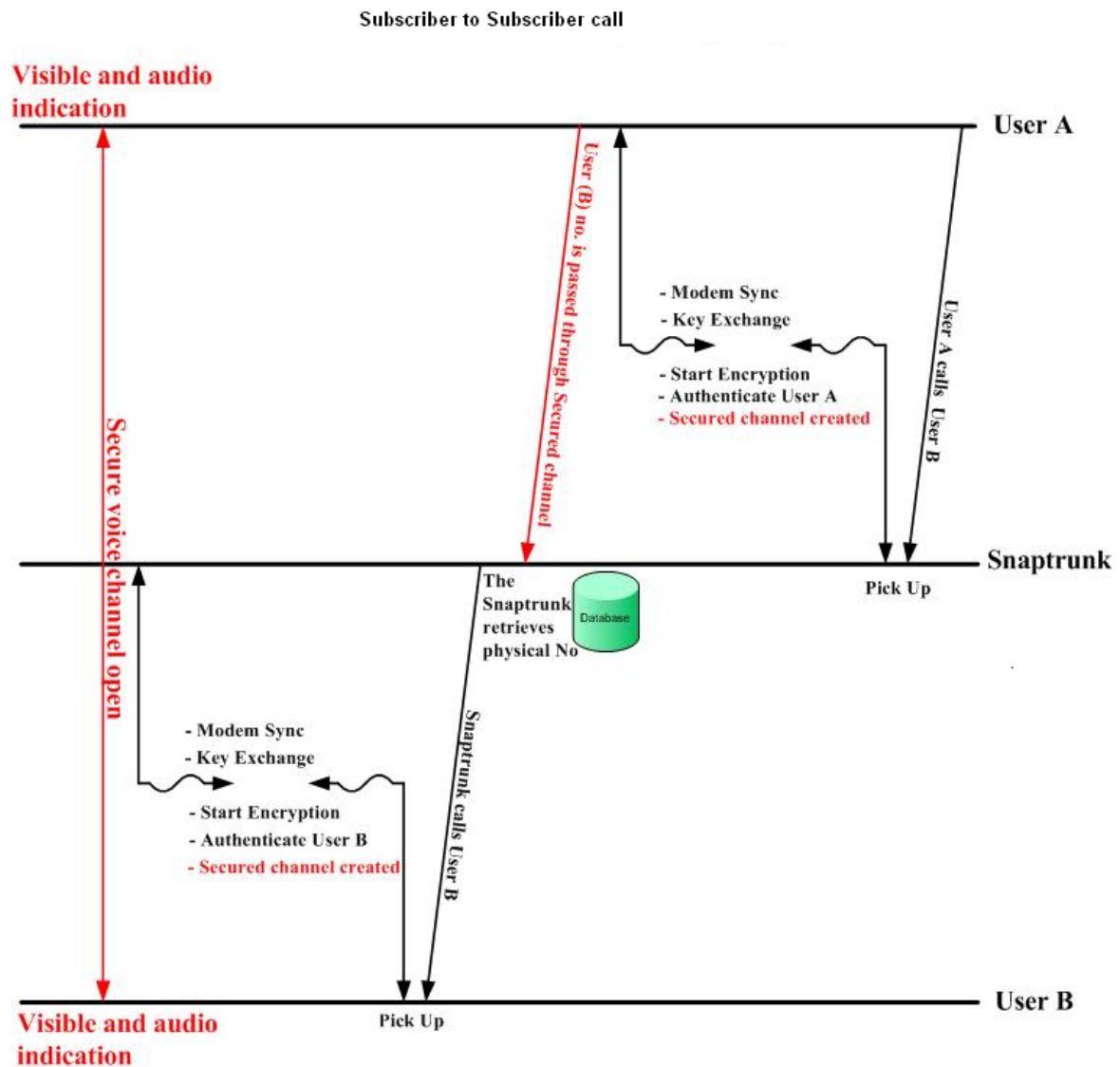
4.4.2 Alert Mechanisms

Email

Phone call through modem

Alert message to **STconsole** (optional feature)

5 Appendix A



6 SnapFense System Specifications

6.1 Snaptrunk Hardware

6.1.1 Snaptrunk Specifications

Industrial-grade PC, Dual Span Dialogic Boards	
Snap Defense Systems Encryption Boards, Network boards	
Hardware Alarm board	
Power Supply	500w (redundant)
Voltage.....	90V ~ 132V, 180V ~ 264V selectable
Frequency.....	47 ~ 63Hz
Current.....	15A@115V, 8A@230V
Power Supply Safety Approval.....	TÜV, UL, CE, FCC
Operating Temperature.....	0 to 50°C
Operating Humidity.....	20-90% RH
Weight.....	40.0 Kg
Dimensions	483(W) x 673(D) x 220(H) mm
Color: Silver, Black	
Network Interface Compliance	according to Dialogic's Global Product Approvals
.....	See http://www.dialogic.com
Power Supply MTBF.....	>100,000 hrs
System Board MTBF.....	100,000 hrs
PSecure MTBF.....	100,000 hrs
Dialogic Network Card MTBF	150,000 hrs
TOTAL MTBF	>27,000 hrs

6.2 Snaptrunk Software

6.2.1 Vocoder

G.723.1 & G.729A	
ADPCM 32	
Voice quality (MOSS).....	3.88 - 4
Bit Rate	6.4Kbps, 8Kbps, 32Kbps

6.2.2 Encryption (FIPS approved)

Diffie-Hellman – Default Prime Number Length	1024 bit
Diffie-Hellman – Default Private Key Length.....	192 bit
3DES (ECB Mode) - Key Length	192 bit
AES - Key Length	256 bit
Total Key Exchange Time	1 sec

6.2.3 Modem

Proprietary Modem	
Maximum Transmission Rate	14,400 bps
Synchronization Time.....	7 sec

6.2.4 V110

According to PRI ISDN standard	
Maximum Transmission Rate	14,400 bps
Synchronization Time.....	7 sec

6.2.5 V32

Maximum Transmission Rate	14,400 bps
Synchronization Time.....	12 sec

6.2.6 Fax Relay

Fax Support.....	GROUP 3 T- 30
------------------	---------------

6.3 Snapfone Hardware

6.3.1 Approvals

FCC Part 15 (Class B)	
CE EMC	EN55022, IEC801-2, IEC801-3, IEC801-4
CE SAFETY	EN60950
Type Approval & Network Compatibility	CTR21

6.3.2 Supported Line Parameters

Line Mode	2 Wire (analog)
Min Ringing Voltage	20 Vrms
Ringing Frequencies	15 to 68 Hz
Loop Current	16 to 40 mA
Loop Current Polarity	any
Line Input Impedance	600 Ω
Max Round Trip Delay Time	1 sec
Intermod 2nd Order Level	40%
Intermod 3rd Order Level	38%
Max Jitter Level	10°
Max Jitter Freq	120 Hz

6.3.3 DTMF Signaling

Table 4 DTMF

Low Group Hz	High Group Hz			
	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Frequencies

Tolerances	$\pm 1.5\%$
Tone Level – High Frequency Group	-9.0 dBV +2.0/-2.5 dB
Tone Level – Low Frequency Group	-11.0 dBV +2.5/-2.0 dB
	when TE Interface terminated with reference impedance Z_R
Tone Level Relativity – High Frequency Group tone higher than Low	1 to 4 dB

6.3.4 Line Interface Parameters (DAA)

AC Line Input Impedance	600 Ω
DC termination (loop current dependent)	$\approx 300 \Omega$ with 60 mA current limitation
Off hook DC Voltage (loop current dependent)	6 to 8 V

6.3.5 Phone Interface Parameters (SLIC)

Open circuit supply	-20 V
Off hook loop current detection	8 mA
On hook loop current detection	7.3 mA
Loop current limitation	30 mA
Maximum load impedance (with loop current of 16 mA)	1000 Ω

6.3.6 Miscellaneous

Power Supply	Dual unregulated DC voltage, 27V/44mA & 7V/600mA
Max Power Consumption	3.5 W
Weight	400 g
Dimensions (HxWxD)	150x45x90 mm
Color Black Operating Temperature	0 to 70°C

6.4 Snapfone Software

6.4.1 Modem

Proprietary Modem
 Maximum Transmission Rate 14,400 bps
 Synchronization Time.....7 sec

6.4.2 Vocoder

G.729A (MOSS).....3.92
 Bit Rate 8Kbps

6.4.3 Encryption (FIPS approved)

Diffie-Hellman – Default Prime Number Length 1024 bit
 Diffie-Hellman – Default Private Key Length..... 192 bit
 3DES (ECB Mode) - Key Length 192 bit
 Total Key Exchange Time 1 sec

6.4.4 Fax Relay

Fax Support GROUP 3 T- 30

6.5 Snapsoft Software

Transmission Rate:.....Network dependent
 Compatibility:.....Windows Mobile 2003 & 2005
 Data Transmission.....Circuit Switched Data 9600 BPS Asynchronous
 Network Data Mode: Transparent & Non-transparent
 Modems:.....v.32 & v.110

Windows Mobile Phones Supported
 HP 6300 Series, Imate K-Jam, Jam, JamIn, PDA2K, Qtek 9100 series

6.5.1 V110

According to PRI ISDN standard
 Maximum Transmission Rate 14,400 bps
 Synchronization Time.....7 sec

6.5.2 V32

Maximum Transmission Rate 14,400 bps
 Synchronization Time..... 12 sec

6.5.3 Fax Relay

Maximum Transmission Rate 14,400 bps
 Synchronization Time..... 12 sec

6.5.4 Vocoder

G.723.1 compliant
 Voice quality (MOSS) 3.88
 Bit Rate 6.4Kbps

6.5.5 Encryption (FIPS compliant)

Diffie-Hellman – Default Prime Number Length 1024 bit
 Diffie-Hellman – Default Private Key Length..... 192 bit
 AES - Key Length 256 bit
 Total Key Exchange Time 1 sec

7 Terminology

ACS	Advanced Calling Services
ANI	Automatic Number Identification
BCC	Billing / Customer Care
BER	Bit Error Rate
CDR	Call Detail Report
CID	Caller Identification
CLASS	Custom Local Area Signaling Services
CO	Central Office
CPE	Customer Premises Equipment
DES	Digital Encryption Standard
DNIS	Dialed Number Identification Service
DSP	Digital Signal Processing
ISDN	Integrated Services Digital Network
LCR	Least Cost Routing
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MIPS	Million Instructions Per Second
MTBF	Mean Time Between Failures
NEBS	Network Equipment Building System
PBX	Private Automatic Branch Extension
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PSTN	Public Switch Telephone Network
RAS	Remote Access Service
SMSC	Short Messaging Service Center
SNAP	Secured Network Access Platform
SnapFense	Managed Interoperable Secure Network
SnapMesh	Wide Area Managed Interoperable Secure Network
Snapcell	Mobile Encryption Device
Snapsoft	Software Security Application
Snapfone	Customer Premises Wireline Encryption Unit
Snaptrunk	Secure Communications Gateway
STconsole	Remote Management Console
Snapgate	Redundant Telco-Grade Security Gateway
Snapmaster	Telco-Grade Multi-server platform
SQL	Microsoft SQL Server
SS No.7	Common Channel Signaling System ITU(T) No.7
VAD	Voice Activated Dialing
VPN	Virtual Private Network